DISTRICT OF COLUMBIA
DEPARTMENT OF INSURANCE AND SECURITIES REGULATION

NOTICE OF FINAL RULEMAKING

The Commissioner of the Department of Insurance and Securities Regulation, pursuant to the authority set forth in § 9 of the Insurer Confidentiality and Information Sharing Amendment Act of 2000, effective October 21, 2000 (D.C. Law 13-191, 47 DCR 7311) and §125 of the Insurance Trade and Economic Development Amendment Act of 2000, effective April 3, 2001 (D.C Law 13-265; D.C. Official Code § 31-2231.25), hereby gives notice of the adoption the following amendments to be included in Chapter 36 of Title 26 of the District of Columbia Municipal Regulations (DCMR). This amendment establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to §§ 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807. This amendment renumbers the section styled "Definitions" currently found at § "3614" to § "3699" with additional terms.

This Notice of Final Rulemaking supercedes the Notice of Proposed Rulemaking published in the D.C. Register on December 20, 2002 at 49 DCR 11451.

Chapter 36 of Title 26 DCMR is amended to read as follows:

3613 INFORMATION SECURITY PROGRAM

3613.1 Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

3614 OBJECTIVES OF INFORMATION SECURITY PROGRAM

3614.1 A licensee's information security program shall be designed to:

(a) Ensure the security and confidentiality of customer information;

(b) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(c) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

3615 EXAMPLES OF METHODS OF DEVELOPMENT AND IMPLEMENTATION

3615.1 Actions and procedures described in §§ 3616 through 3619 of these rules are examples of methods of implementation of the requirements of §§ 3613 and 3614 of this regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement §§ 3613 and 3614 of these rules.

3616 ASSESS RISK

3616.1 The licensee shall:

(a) Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

(b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(c) Assess the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

3617 MANAGE AND CONTROL RISK

3617.1 The licensee shall:

(a) Design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(b) Train staff, as appropriate, to implement the licensee's information security program; and

(c) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

3618 OVERSEE SERVICE PROVIDER ARRANGEMENTS

3618.1 The licensee shall:

(a) Exercise appropriate due diligence in selecting its service providers; and

(b) Require its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

3619 ADJUST THE PROGRAM

3619.1 The licensee shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

3620 DETERMINED VIOLATION

3620.1 Violation of these rules shall constitute an unfair trade practice under § 101(9) of the Insurance Trade and Economic Development Amendment Act of 2000, effective April 3, 2001 (D.C. Law 13-265, D.C. Official Code §31-2231.01(9)).

3621-3698 RESERVED

3699 DEFINITIONS

Customer information means the same as nonpublic personal information, and applies whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

Customer information systems means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

Service provider means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.